MULTIMEDIA UNIVERSITY

STUDENT ID NO

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 2, 2015/2016

ECE3246 – SECURITY & CRYPTOGRAPHY

(CE, ME)

8 MARCH 2016
9:00 a.m. - 11.00 a.m.
(2 Hours)

INSTRUCTIONS TO STUDENT

1. This examination paper consists of 6 pages including the cover page with 4 questions only.
2. Attempt **any THREE** out of **FOUR** questions. All questions carry equal marks and the distribution of the marks for each question is given.
3. Please print all your answers in the Answer Booklet provided.

Question 1

a) Describe the two **security properties** known as *source authentication* and *message integrity*. Explain how each can be offered by a digital signature scheme.

[3+3 marks]

b) Consider the MixColumns operation within a round of Mini-AES, wherein multiplication of two nibbles is to be performed modulo a primitive polynomial $m(x) = x^4+x+1$. Show how the **multiplication** of 0101 and 1101 can be done modulo $m(x)$.

[6 marks]

c) (i) Discuss whether a block cipher can be used to achieve the security goal of **integrity** (INT).

[3 marks]

(ii) Given that two parties A and B wish to engage in the communication of a message m, across a public channel where an adversary Z has access to. Discuss in some detail (i.e. in terms of what the sender does, what the recipient should be able to do and what the adversary should not be able to do) the main approach for A and B to achieve **integrity** (INT) between them.

[5 marks]

Question 2

a) Describe how a public key infrastructure (PKI) enables to achieve confidentiality (CONF) and source authentication (AUTH).

[3+3 marks]

b) Discuss the similarities and differences between the KR-CCA and IND-CCA security models of encryption.

[3+3 marks]

Continued...

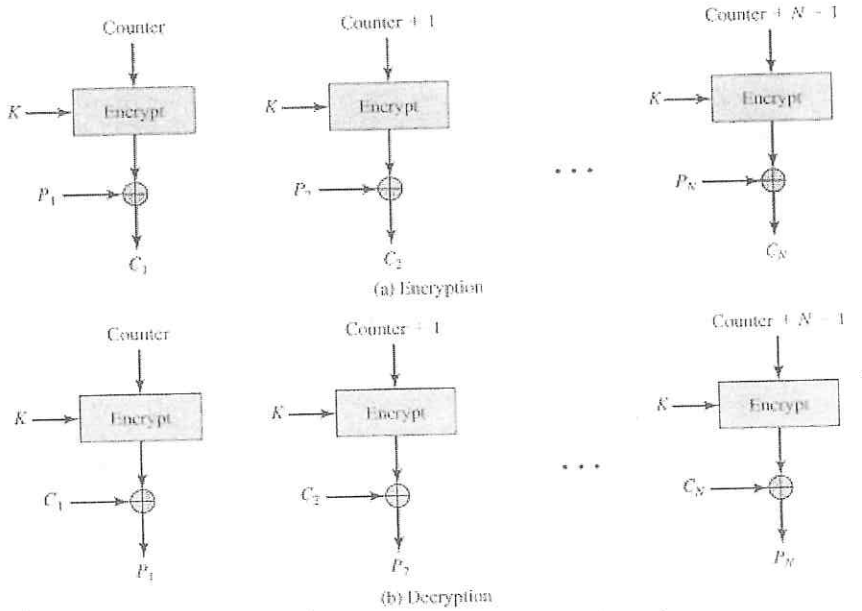

Figure 1 [sourced from Stallings book]

c) Figure 1 shows a way in which a block cipher E can be used, where counter can be seen to be a counter variable that is incremented at each iteration.

(i) Discuss *what security* property can be achieved, and *why* it can be achieved, when a block cipher is used in this way. [4 marks]

(ii) Discuss whether the cut-&-splice attack can work, giving your reasons. [4 marks]

Question 3

a) (i) The *discrete log problem* aims to determine x when given $X = g^x \bmod p$ and where the base g and modulus p are also known. Describe the basic idea why this problem is mathematically infeasible for large integers. [3 marks]

(ii) Explain what is one basic approach that relates the **security** of a cryptographic scheme to the hardness of solving the discrete log problem. [3 marks]

Continued...

b) The RSA public key cipher performs encryption defined as follows

$c = m^e \bmod n$

where c is the ciphertext, m the plaintext, e the public key and n the modulus, and decryption is defined as

$m = c^d \bmod n$.

With some appropriate symbols, notations and/or examples, show why the RSA is homomorphic. [6 marks]

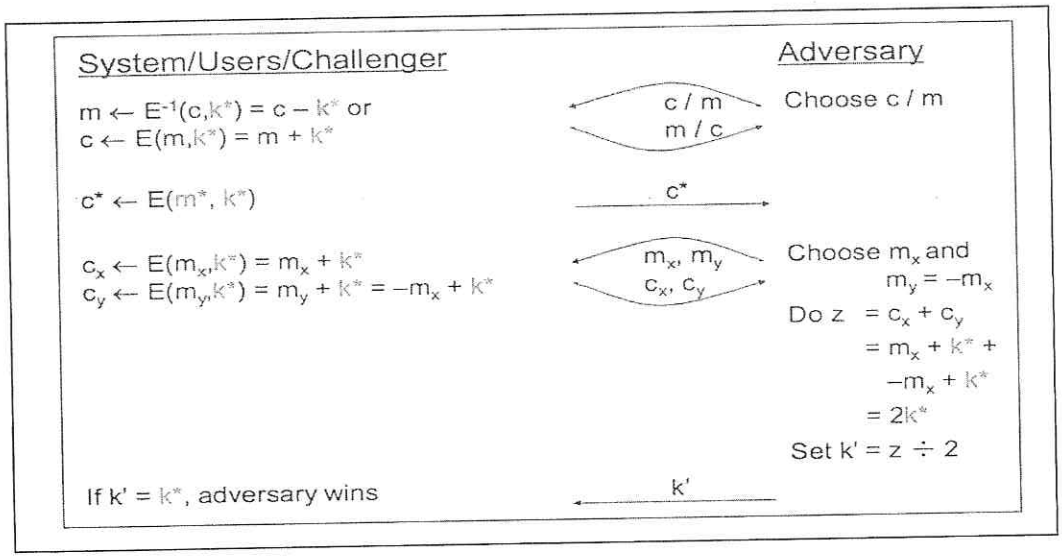
System/Users/Challenger
Adversary
m ← E⁻¹(c,k*) = c – k* or
c ← E(m,k*) = m + k*
c / m
m / c
Choose c / m
c* ← E(m*, k*)
c*
c_x ← E(m_x,k*) = m_x + k*
c_y ← E(m_y,k*) = m_y + k* = –m_x + k*
m_x, m_y
c_x, c_y
Choose m_x and
m_y = –m_x
Do z = c_x + c_y
= m_x + k* +
–m_x + k*
= 2k*
Set k' = z ÷ 2
If k' = k*, adversary wins
k'

Figure 2

c) Figure 2 shows an attack by an adversary against the AddCipher in the security model called the key-recovery against chosen-ciphertext attacks (KR-CCA) model.

(i) Discuss whether oracles are being exploited by the adversary. [4 marks]

(ii) Discuss what is the main strategy used by the adversary in achieving his goal. [4 marks]

Continued...

Question 4

a) (i) Explain your understanding of what is a virtual private network (VPN). [3 marks]

(ii) Describe what you understand by the concept of perfect forward secrecy (PFS) and why it is important for security. [3 marks]

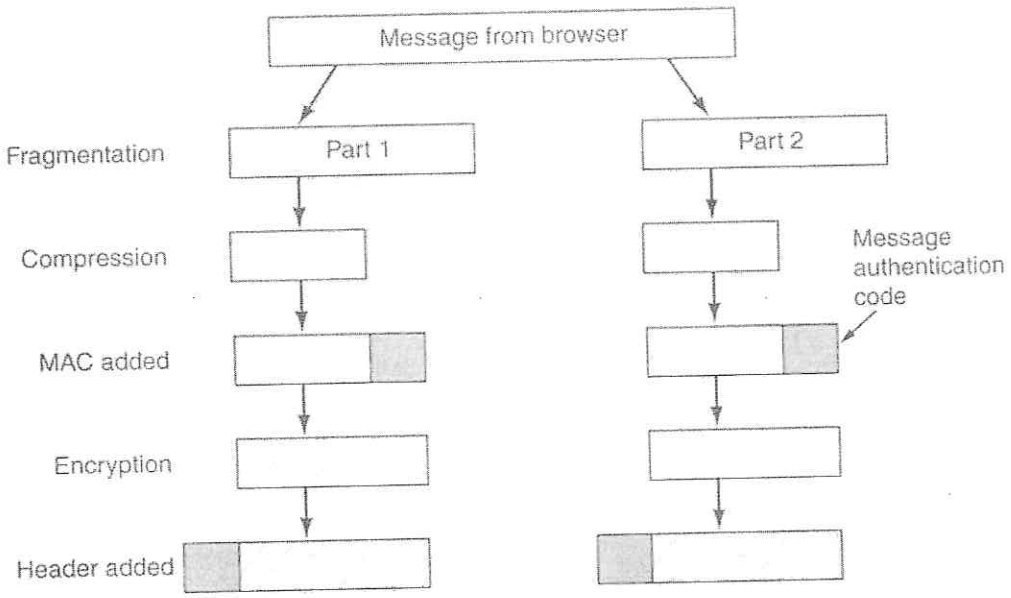

Figure 3

b) (i) Figure 3 shows the process of combining encryption with a message authentication code (MAC). Why should compression be performed first before these two operations? [2 marks]

(ii) Explain what happens at the recipient side when the compressed / MACed / encrypted message is received. [4 marks]

Continued...

(1) Alice → Bob : g^x
(2) Alice ← Bob : g^y, $E_K(S_B(g^y, g^x))$
(3) Alice → Bob : $E_K(S_A(g^x, g^y))$

Figure 4

c) Figure 4 shows a variant of the Diffie-Hellman Key Exchange (DHKE) protocol known as the Station-to-Station (STS) protocol where K is the shared key between Alice and Bob, $E_K( )$ denotes symmetric encryption using key K, and $S_A( )$ denotes a digital signature signed by Alice.

(i) Explain what is achieved by the functions $E_K( )$ and $S_A( )$ within the context of the STS protocol. [3 marks]

(ii) Discuss the security of this STS protocol against *either* the replay attack or the man-in-the-middle attack. [5 marks]

End of Paper